PCT / IB 04 / 01981
10 JUN 2004

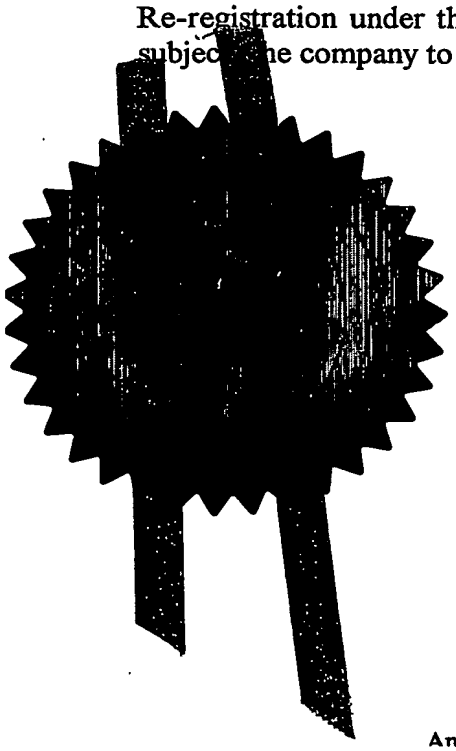
The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.



Signed

Dated 15 March 2004

Patents Form 1/77

P[redacted]ct 1977
(Ru[redacted])

THE PATENT OFFICE
21 JUN 2003
NEWPORT

The Patent Office

1/77

Request for grant of a patent

(See notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office
Cardiff Road
Newport
Gwent NP10 8QQ

Your reference — PHGB030099GBP — 21 JUN 2003

Patent application number
(The Patent Office will fill in this) 0314562.0

ZJJAN03 E816989-2 D03008
P01/7700 0.00-0314562.0

Full name, address and postcode of the or of each applicant (*underline all surnames*)

KONINKLIJKE PHILIPS ELECTRONICS N.V.
GROENEWOUDSEWEG 1
5621 BA EINDHOVEN
THE NETHERLANDS

Patents ADP Number (*if you know it*) — 07419294001

If the applicant is a corporate body, give the country/state of its incorporation — THE NETHERLANDS

Title of the invention — IMPROVED INVERSION CALCULATIONS

Name of your agent (*if you have one*)
"Address for service" in the United Kingdom to which all correspondence should be sent (*including the postcode*)

Philips Intellectual Property and Standards
Cross Oak Lane
Redhill
Surrey RH1 5HA

Patents ADP number (*if you know it*) — 08359655001

If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and (*if you know it*) the or each application number	Country	Priority Application number (*if you know it*)	Date of filing (*day/month/year*)

If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application	Number of earlier application	Date of filing (*day/month/year*)

Is a statement of inventorship and of right to grant of a patent required in support of this request? (*Answer "Yes" if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.

See note (d))

YES

Enter the number of sheets for any of the following items you are filing with this form.
Do not count copies of the same document.

Continuation sheets of this form	
Description	10
Claims(s)	3
Abstract	1
Drawings	7

If you are also filing any of the following, state how many against each item:

Priority Documents

Translations of priority documents

Statement of inventorship and right to grant of a patent (*Patents Form 7/77*)

Request for preliminary examination and search (*Patents Form 9/77*)

Request for substantive examination (*Patents Form 10/77*)

Any other documents (*Please specify*)

I/We request the grant of a patent on the basis of this application.

Signature Richard Turner Date 20.6.3

Name and daytime telephone number of person to contact in the United Kingdom 01293 815492 (R. Turner)

ırning

er an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or nmunication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be ɔrmed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, :tion 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the :ent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same ention and either no direction prohibiting publication or communication has been given, or any such direction has been oked.

tes

If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.

Write your answers in capital letters using black ink or you may type them.

If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.

If you have answered "Yes" Patents Form 7/77 will need to be filed.

Once you have filled in the form you must remember to sign and date it.

For details of the fee and ways to pay please contact the Patent Office.

DESCRIPTION

IMPROVED INVERSION CALCULATIONS

The present invention relates to a method of performing an inversion operation and to apparatus for performing an inversion operation.

Elliptic Curve Cryptography (ECC) involves the use of calculations on an elliptic curve relationship over GF(p) or GF(2^n)and requires the multiplication of long integers which are carried out repeatedly during the implementation of, for example, public key algorithms in cryptographic processors.

Typically, the multiplication operations must be carried out many hundreds of times to complete an encryption or decryption operation, and so it is important that the cryptographic devices that perform these operations execute the long multiplications quickly using a high speed multiplier.

ECC calculations require also an inversion calculation, i.e. the calculation of Z^{-1}, such that the product $Z.Z^{-1}=1$ mod N. Every point addition and point doubling calculation requires such a calculation. The present algorithms are computational intensive.

Another way is working in the so-called Projective Space. This postpones the inversion calculation to the end and has to be done only once, but the trade-off is that the number of multiplications is largely increased.

Increasingly, such cryptographic algorithms are used in electronic devices for example smart cards, and in these applications processing capability and power consumption is severely limited.

One conventional calculation method is the binary GCD system which works with pairs of auxiliary variables. One pair is reduced in size by dividing by 2 when even, or by subtracting when odd.

However, in the GCD system often it is necessary to correct the operation on the other pair by the addition of half of the modulus.

Another conventional calculation method is the Kaliski system which again uses two pairs of auxiliary variables, of which one pair is reduced by dividing by 2 when even, or by subtracting when odd.

However, in this system, any required correction is delayed to the second stage.

It is therefore an object of the present invention to provide a more efficient inversion operation.

It is also an object of the present invention to provide a inversion process with fewer operations.

It is also an object of the present invention to provide an inversion operation which is completed faster than in conventional systems.

According to one aspect, the present invention provides a method of performing an inversion operation in a cryptographic calculation with at least two auxiliary variables, the method comprising shifting a variable, then effecting a reduction by subtracting that variable from a larger variable.

One advantage of the present invention is that most operations are only done on the Most Significant Words of the auxiliary variables. After a number of such computations, a number of multiplications are done on the complete auxiliary variables, which are simpler.

These advantages result in the number of necessary operations being reduced as compared to conventional methods, thereby ensuring that the calculations can be effected more quickly.

Thus a significant benefit provided by the present invention is that the time taken to complete the entire calculating operation is reduced.

Moreover, the degree of security afforded by the method of the present invention is maintained as compared to conventional cryptographic methods.

Preferably, the method comprises four auxiliary variables being U, V, R and S having the invariances:-

$|S.V-R.U| = N$

$S.Y = U \bmod N$

$R.Y = V \bmod N.$

Preferably, the method operates with the Most Significant Words of the variables.

Thus an advantage of the present invention is that the calculation operations are effected faster.

According to another aspect, the present invention provides a computer program product directly loadable into the internal memory of a digital computer, comprising software code portions for performing the method of the present invention when said product is run on a computer.

According to another aspect, the present invention provides a computer program directly loadable into the internal memory of a digital computer, comprising software code portions for performing the method of the present invention when said program is run on a computer.

According to another aspect, the present invention provides a carrier, which may comprise electronic signals, for a computer program embodying the present invention.

According to another aspect, the present invention provides electronic distribution of a computer program product, or a computer program, or a carrier of the present invention.

According to another aspect, the present invention provides apparatus for performing an inversion operation in a cryptographic calculation with at least two auxiliary variables, the apparatus comprising means to shift a variable, and means to effect a reduction by subtraction or addition of that variable from a larger variable.

The method and apparatus of the present invention is applicable to calculations over GF(p), GF(2^n) and also long-integer division.

In order that the present invention may more readily be understood, a description is now given, by way of example only, reference being made to the accompanying drawings, in which:-

Figure 1 is a block diagram of an application of the invention in a smart card;

Figure 2 is a schematic drawing of an inversion operation embodying the present invention;

Figure 3 is a hardware implementation of the present invention;

Figure 4 is a further detailed hardware implementation of the present invention;

Figure 5 is a schematic drawing of another inverse operation of the present invention;

Figure 6 is a schematic drawing of another inverse operation of the present invention;

Figure 7 is a schematic drawing of a further operation of the present invention.

Figure 1 shows a block diagram of a hardware implementation of the present invention incorporating a smart card 50 with the following components:

- Microcontroller 51 for general control to communicate with the outside world via the interface. It sets pointers for data in RAM/ROM and starts the coprocessor.
- Interface to the outside world, for contact with smart cards e.g. according to ISO-7816-3.
- A Read Only Memory (ROM) 52 for the program of the microcontroller.
- A Programmable Read Only Memory (Flash or EEPROM) 53 for the non-volatile storage of data or programs.
- RAM 54 for storage of volatile data, e.g for storage of intermediate results during calculations.
- Coprocessor 55 dedicated to perform special high-speed tasks for ECC or RSA calculations. When a task is ready, control is returned to the microcontroller.

In a variant, the present invention is implemented in software with a microprocessor, ALU to provide add, subtract, shift operations with programming of the controller to provide control logic, and degree detection by shift registers. 2

There is shown in Figure e an inversion operation of the present invention which is described below.

Thus this method of calculation over GF(p) involves the operation

$R = Y^{-1} \bmod N$

having four auxiliary variables U, V, S and R, with

$U = Y$

$V = N$

$S = 1$

$R = 0$,

U and V always being positive.

The degree of an auxiliary variable is the number of relevant bits to represent it. Thus for example, if U = 111100

then the degree of U = dU is 6;

and, if V = 001110,

then the degree of V = dV is 4.

The operation involves taking:

$B = dU - dV$ (Step S1);

and, if b<0, then performing the operations (Step S2, S3):-

(swap U, V)

(swap R, S)

(swap dU, dV)

$b = -b$

then $U = U - 2^b.V$

$S = S - S^b.R$

and if (U< 0)

then (Step S4) U = - U

$S = -S$,

if (R<0), then R = R+N

if (R>N), then R = R-N.

Thus the following invariants hold after each loop iteration:

$\gcd(U,V) = \gcd(Y,N)$

$SY = U \bmod N$

$RY = V \bmod N$

$|SV-RU| = N$.

In every step, either the degree of U is decreased or the degree of V. Therefore U and V become smaller and smaller, until in the last step U becomes 0 ($U=2^bV$).

Since U= 0, the invariance gcd(U,V)=gcd(Y,N) implies V=gcd(Y,N)=1, since Y and N are relative prime.

Then RY=1 mod N or $R = Y^1$ mod N.

When U= 0, -N<R<2N,

giving at most one correction step namely: either adding or subtracting N.

In practice, R appears always to be smaller than N, so that subtraction of N never occurs.

Also, |SV|<2N and |RU|<2N temporary.

Since they are all integers,

|S|<2N;

|V|<2N;

|R|<2N;

|U|<2N.

For these variables, only one bit more than N requires representing them. For S and R, a sign-bit is needed too.

Figure 2 shows the hardware implementation of the method of the present invention.

Registers 10, 11, 12 and 13 hold variables U, V, S, R. The adders 14, 15 perform addition, subtraction, negation and mod 2 additions. V and R can be shifted over b bits. The control logic 16 controls the process. There are two degree detectors 17,18, one for U and one for V. The dSubtractor 19 gives the difference (b).

Initially, Y is loaded into U, N into V, S is set to 1 and R to 0.

Then the process is started.

When b<0, U and V exchange their contents, S and R do the same, and b is negated.

Both adders are set to subtraction and the shifters are set to shift over b bits. Then the subtraction is performed. When U is negative, the adders are set to negate both U and S.

The process is done as long as $U \neq 0$.

When $U=0$ and $R<0$ or $R>N$, S is loaded with N. Then either R+N or R-N is calculated.

Normally, the operands consist of a number of words. However, in a variant, the calculations can be speeded up by using only the Most Significant Word two of the variables and 4 auxiliary variables with the size of 1 word, while keeping the invariances valid. It saves also chip area and power. The result is used as an estimator for the subsequent calculation on the whole operands.

Figure 3 shows the more detailed hardware implementation . Registers 30 to 35, each with a 1 word capacity, hold U_H,V_H,uu, uv, vu and vv.

U_H and V_H are initially loaded with the Most Significant Word of U and V.

$U = uu.U_0 - uv.V_0$

$V = vu.U_0 - vv.V_0$

$S = uu.S_0 - uv.R_0$

$R = vu.S_0 - vv.R_0$

uu,uv vu and vv are words of convenient size.

The operation starts with uu=1, vv=-1 and uv=vu=0,

$U_0 = Y;$

$V_0=N;$

$S_0=1;$

$R_0=0.$

Assume that the equations are still correct after a number of steps. After the next calculation, the equations are still correct. Since they are correct in the beginning, they remain correct.

When calculating $U' = U-2^bV$ and $S'= S-2^bR$, then choose:

$uu'=uu-2^bvu$

$uv'=uv-2^bvv$

$vu'=vu$

$vv'=vv.$

When it is necessary to calculate $U'=U+2^bV$ and $S'=S+2^bR$, then choose:

$uu'=uu+2^b vu$

$uv'=uv+2^b vv$

$vu'=vu$

$vv'-vv$.

When required, swap uu and vu; uv and vv.

This swaps U and V as well R and S.

To update the operands, start with loading U_H with MSW of U and V_H with the MSW of V. Then,

uu=1,vv=-1 and uv=uv=0.

Then a number of calculations are done, the amount depending on the size of the words and how many useful bits are left over.

Since V_H is shifted, it is supplemented with zeros instead of the (unknown) right bits so U_H and V_H become smaller and smaller. The operation is halted when there are almost no bits left. Also the determination of the sign become incorrect.

Then calculate U, V, S and R by means of uu...vv and $U_0...S_0$.

This gives new reduced values of U and V, which still obey the invariance.

Then set U_0 to U, V_0 to V and the same for S_0 and R_0. Again set uu=1, vv=-1 and uv=vu=0.

Then repeat the procedure. Every time U and V become smaller and smaller, until they fit in the U_H and V_H registers.

Then the calculation is no longer an estimation, but an exact calculation and it ends with the correct result. Finally, only R has to be recalculated to find Y^{-1}

In a variant to the method of Figures 1 to 4, the calculation method allows negative values for U and V and removes the correction step when U is negative (see Figure 5).

The degree of positive numbers is the number of bits after removing all leading zeroes and the degree of negative numbers is the number of bits after removing all leading ones.

Again, the auxiliary variables are:

U=Y;

V=N;

S=1;

R=0;

while (U≠0) and

if (b<0) then effect:

{swap (U,V); swap (R,S) swap(dU,dV); b=-b};

if (Sign(U)=Sign(V))

then effect

{$U=U-2^b.V$;$S=S-2^b.R$;}

Else

{$U=U+2^b.V$; $S=S+2^b.R$;}

dU=degree(U);

if (R<0), then R=R+N;

if (R>N) then, R=R-N.

Figure 6 shows a second embodiment which is a calculation method over GF(2^n), the major differences being:

α is the variable of the polynomials, U, V, S and R;

N is the irreducible polynomial;

the algorithm is simpler since there are no negative values and there is only a mod 2 addition.

Thus with

U=Y;

V=N;

S=1;

R=0;

while (U>0)

b=dU-dV

if (b<0) {swap(U,V);swap(R,S); swap(dU,dV); b=-b;}

$U=U\oplus\alpha^b.V$;

$S=S\oplus\alpha^b.R$;

d=degree(U);

if (R>N) R=R⊕N.

Thus, initially, Y is loaded into U, N into V, S is set to 1 and R to 0.

Then the process is started (Steps S10-S12).

When b<0, U and V exchange their contents, S and R do the same and b is negated.

Both adders are always set to add mod 2. The shifters are set to shift over b bits. Then the addition is performed.

The process is done as long U≠0

When U=0 and R=R>N, S is loaded with N, then R ⊕ N is calculated.

Figure 7 shows a third embodiment which is a calculation method for long-integer division, the major differences being:

Initially, X is loaded into U, Y into V, S is set to 0 and R to 1.

When U>0, then the UV–adder is set to subtraction and the RS-adder to addition, or the reverse is done, as appropriate. The shifters are set to shift over b bits. Then the addition/subtraction operation is performed.

The process is done for as long U≠0 and b≥0.

When the process is ready and U<0, then b is set to 0. Then one addition/subtraction is performed (U=U+V; S=S-R).

Then U is the remainder R' and S is the quotient Q, X = Q.Y+R' with 0≤R'<Y.

CLAIMS

1. A method of performing an inversion operation in a cryptographic calculation with at least two auxiliary variables, the method comprising shifting (S2) a variable, then effecting a reduction (S3) by subtracting that variable from a larger variable.

2. A method according to Claim 1 wherein the variables are of the same degree.

3. A method according to Claim 1 or 2 comprising updating a plurality of additional variables such that the invariances remain valid.

4. A method according to any preceding claim comprising four auxiliary variables being U, V, R and S, having the invariances:

$|S.V-R.U| = N$

$S.Y = U \bmod N$

$R.Y = V \bmod N$.

5. A method according to Claim 4 comprising decreasing U and V in size, step by step until U = 1.

6. A method according to Claim 5 comprising effecting the operation $R.Y = 1 \bmod N$ or $R = Y^{-1} \bmod N$, as appropriate.

7. A method according to any preceding claim comprising operating with the Most Significant Words of the variables.

8. A method according to any preceding claim comprising providing inversion (S1-S4) over GF(p).

9. A method according to any preceding claim comprising providing inversion (S10-S12) over GF(2^n).

10. A method according to any preceding claim comprising providing a method for long-integer division operations.

11. A computer program product directly loadable into the internal memory of a digital computer, comprising software code portions for performing the method of any one or more of Claims 1 to 10 when said product is run on a computer.

12. A computer program directly loadable into the international memory of a digital computer, comprising software code portions for performing the method of any one of Claims 1 to 10 when said program is run on a computer.

13. A carrier, which may comprise electronic signals, for a computer program of Claim 12.

14. Electronic distribution of a computer program product of Claim 11 or a computer program of Claim 12 or a carrier of Claim 13.

15. Apparatus for performing an inversion operation in a cryptographic calculation with at least two auxiliary variables, the apparatus comprising means to shift a variable (V, R) and means (10-17) to effect a reduction by subtraction or addition of that variable from a larger variable.

16. Apparatus according to Claim 15 wherein the variables (V, R) are of the same degree without shifting.

17. Apparatus according to Claim 15 or 16 comprising means to update a plurality of additional variables such that the invariance remains valid.

18. Apparatus according to any of Claims 15 to 17 comprising means (10-13) to operate four auxiliary variables being U, V, R and S, having the invariances:

$|S.V-R.U| = N$

$S.Y = U \bmod N$

$R.Y = V \bmod N.$

19. Apparatus according to Claim 18 comprising means (10, 11) to decrease U and V in size, step by step until U = 1.

20. Apparatus according to Claim 19 comprising means (10-16) to effect the operation $R.Y = 1 \bmod N$ or $R = Y^{-1} \bmod N$, as appropriate.

21. Apparatus according to any of Claims 15 to 20 comprising means to operate with the Most Significant Words of the variables.

22. Apparatus for performing an inversion operation in a cryptographic calculation substantially as hereinbefore described with reference to, and/or as illustrated in, any one or more of the Figures of the accompanying drawings.

23. A method of performing an inversion operation in a cryptographic calculation substantially as hereinbefore described with reference to, and/or as illustrated in, any one or more of the Figures of the accompanying drawings.

ABSTRACT

IMPROVED INVERSION CALCULATIONS

An Elliptic Curve Crypography inversion technique utilises operating on the MSW of four auxiliary variables U, V, R and S with specified invariences.

[Figure 3]

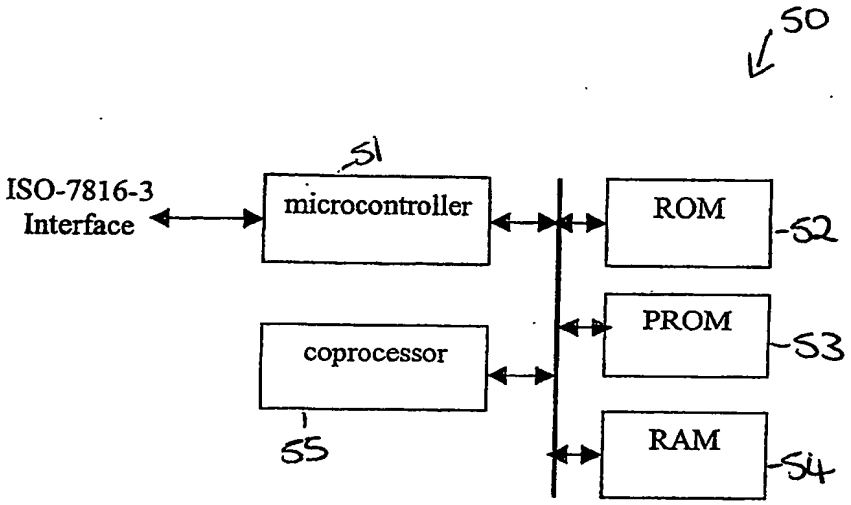

50
51
ISO-7816-3
Interface
microcontroller
ROM
52
PROM
53
coprocessor
55
RAM
54

Figure 1

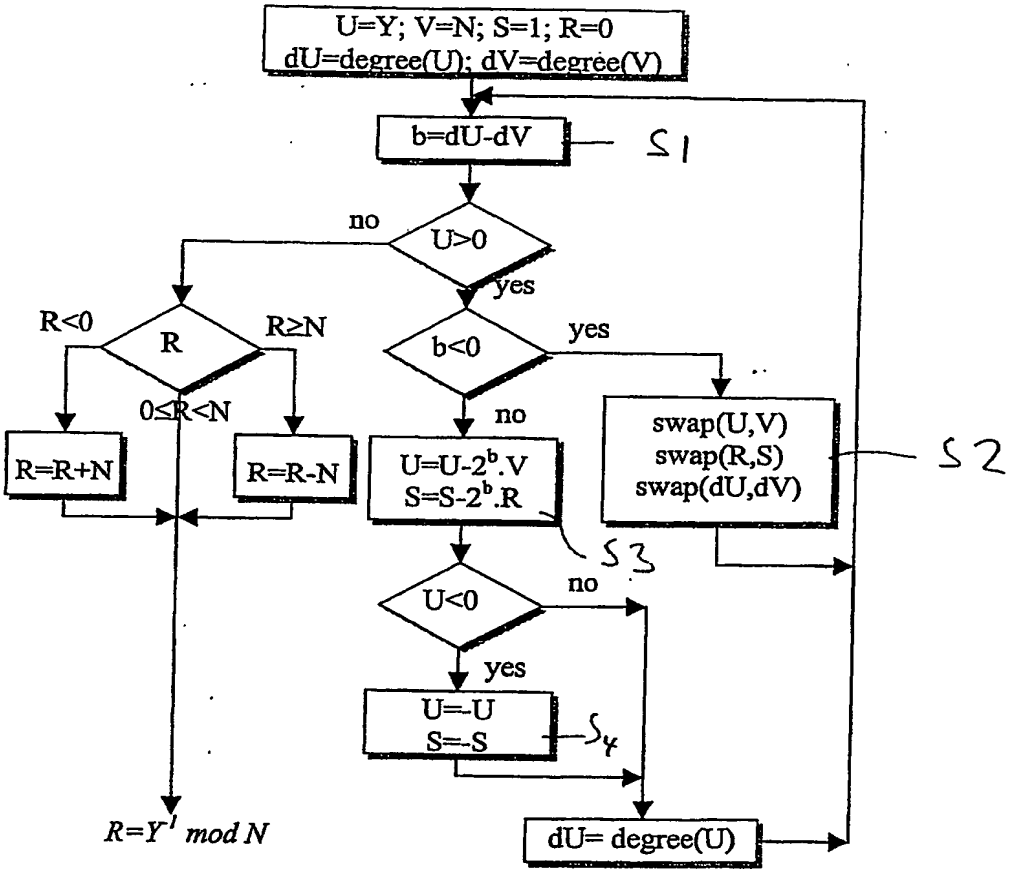

U=Y; V=N; S=1; R=0
dU=degree(U); dV=degree(V)
b=dU-dV
S1
no
U>0
yes
R<0
R
R≥N
0≤R<N
b<0
yes
no
swap(U,V)
swap(R,S)
swap(dU,dV)
S2
R=R+N
R=R-N
U=U-2^b.V
S=S-2^b.R
S3
U<0
no
yes
U=-U
S=-S
S4
R=Y^l mod N
dU= degree(U)

Figure 2

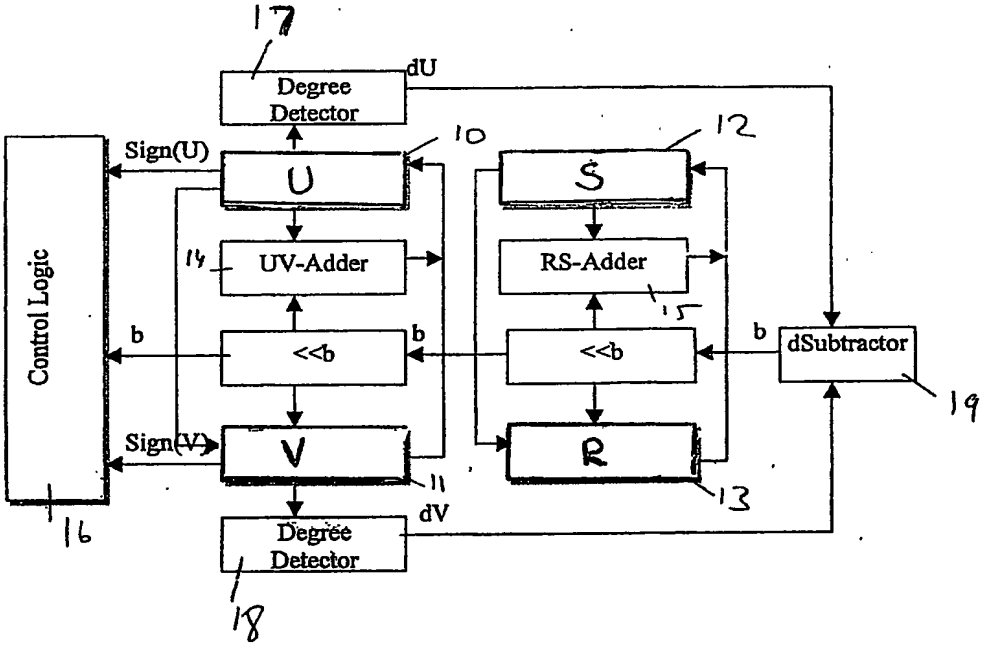

17
Degree Detector
dU
Sign(U)
U
10
S
12
Control Logic
14
UV-Adder
RS-Adder
15
b
<<b
b
<<b
b
dSubtractor
19
Sign(V)
V
11
R
13
dV
16
Degree Detector
18

Figure 3

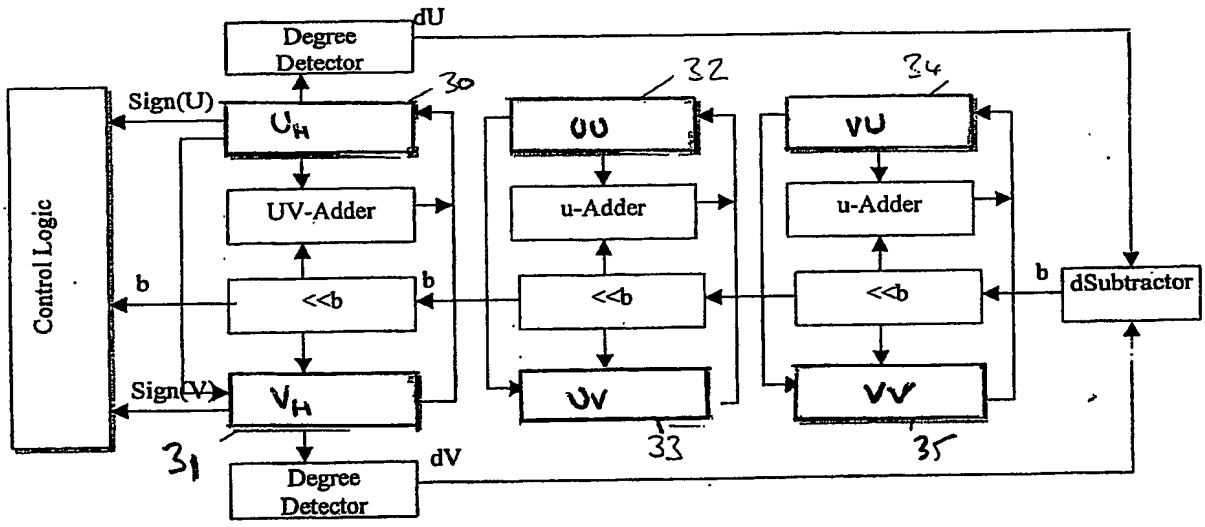

Degree Detector
dU
Sign(U)
30
32
34
Control Logic
UH
UU
VU
UV-Adder
u-Adder
u-Adder
b
<<b
b
<<b
<<b
b
dSubtractor
Sign(V)
VH
UV
VV
31
33
35
dV
Degree Detector

Figure 4

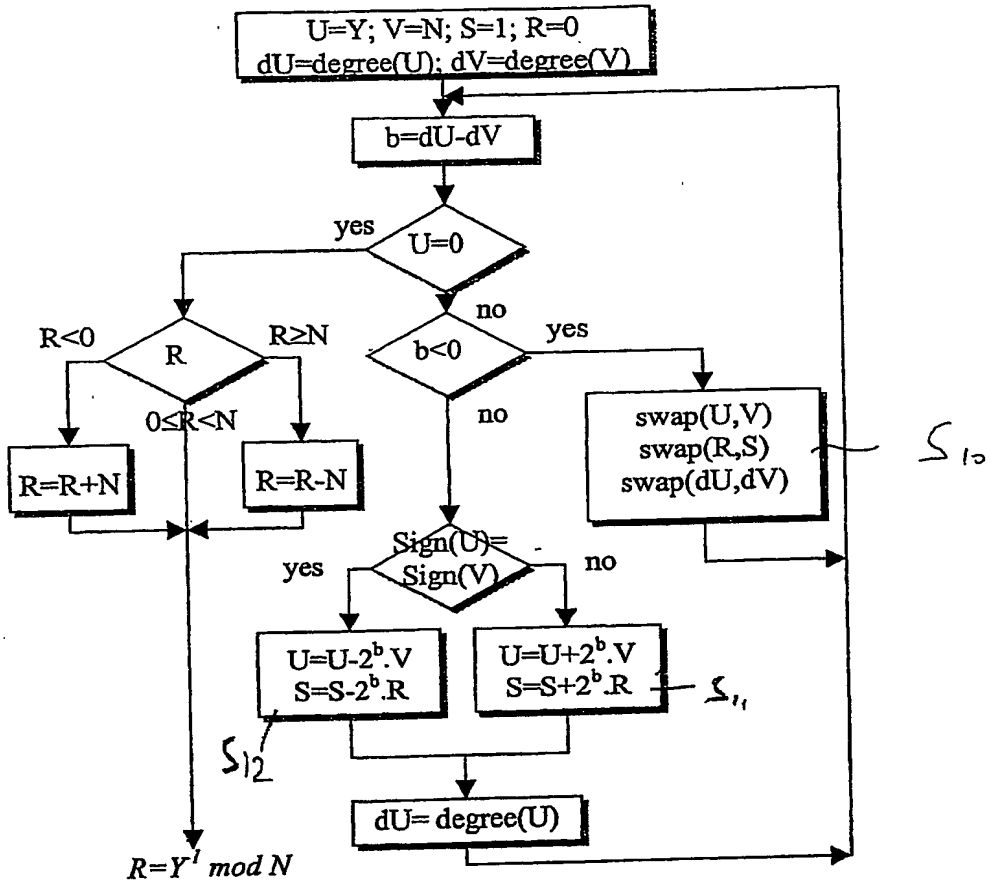

U=Y; V=N; S=1; R=0
dU=degree(U); dV=degree(V)
b=dU-dV
yes
U=0
no
R<0
R
R≥N
b<0
yes
no
0≤R<N
swap(U,V)
swap(R,S)
swap(dU,dV)
S10
R=R+N
R=R-N
Sign(U)=
Sign(V)
yes
no
U=U-2^b.V
S=S-2^b.R
U=U+2^b.V
S=S+2^b.R
S11
S12
dU= degree(U)
R=Y^-1 mod N

Figure 5

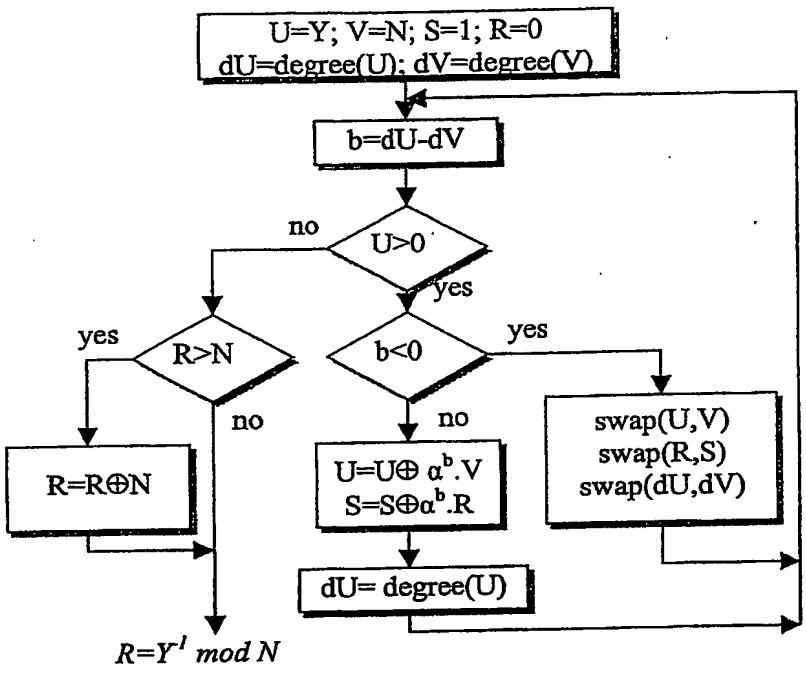

U=Y; V=N; S=1; R=0
dU=degree(U); dV=degree(V)
b=dU-dV
no
U>0
yes
yes
R>N
b<0
yes
no
no
R=R⊕N
U=U⊕ α^b.V
S=S⊕α^b.R
swap(U,V)
swap(R,S)
swap(dU,dV)
dU= degree(U)
R=Y^l mod N

Figure 6

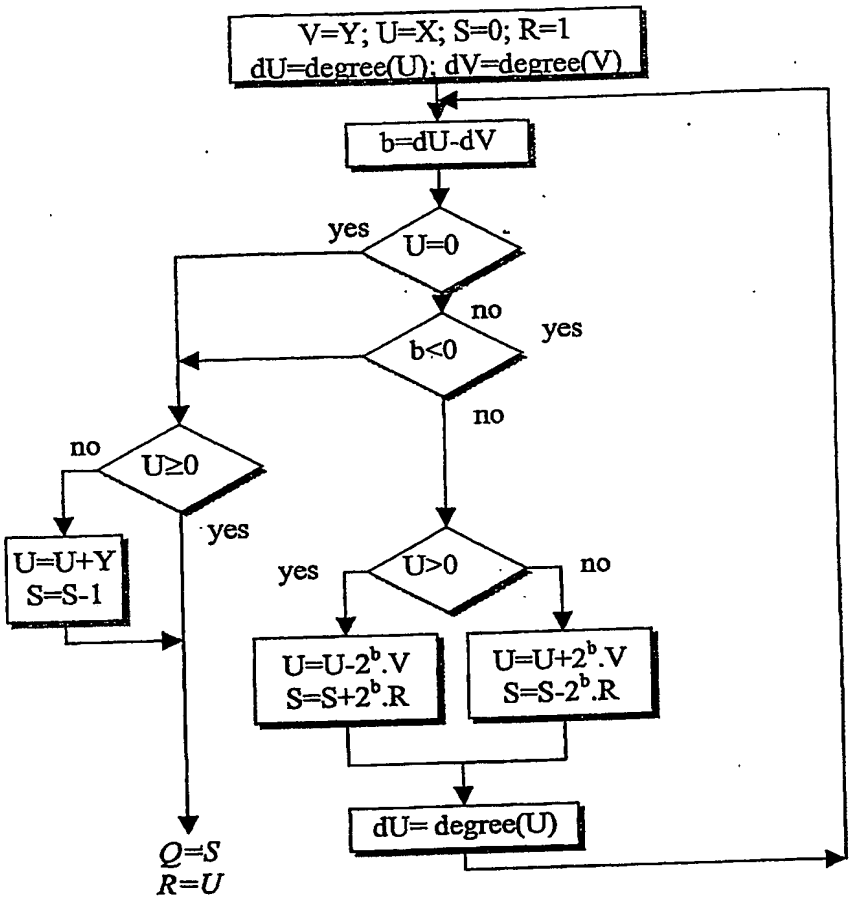

V=Y; U=X; S=0; R=1
dU=degree(U); dV=degree(V)
b=dU-dV
yes
U=0
no
b<0
yes
no
no
U≥0
yes
U=U+Y
S=S-1
yes
U>0
no
U=U-2^b.V
S=S+2^b.R
U=U+2^b.V
S=S-2^b.R
dU= degree(U)
Q=S
R=U

Figure 7